



MORGAN HILL POLICE DEPARTMENT

16200 Vineyard Blvd., Morgan Hill, CA 95037 Office: (408)779-2101 Fax: (408)776-7328

Identity Theft

What to do if you are a victim:

- Keep records of your conversations and correspondence with creditors, collection agencies, financial institutions, government agencies, etc.
- Call the Federal Trade Commission's Identity Theft Hotline:
(877) 438-4338
- Counselors will assist you with resolving identity theft issues.
- Contact the three credit bureaus to report incidents of fraud or theft of your identity.
- Place a "fraud alert" on your credit record.
 - Equifax (800) 525-6285
 - Experian (888) 397-3742
 - Trans Union (800) 680-7289

Some bureaus may offer you a free copy of your credit report. If not, purchase one. Carefully review the report.

- Notify the credit bureau(s) of any fraudulent accounts or charges, in writing, within 30 days.
- Review your credit report every few months for a period of one year.
- Notify the creditor(s) reporting you as delinquent that you have been a victim of fraud.
- Call by phone to report the fraud and close the fraudulent account.
- Follow-up your initial dispute in writing to preserve your rights as a victim of credit fraud.
- File an identity theft report with the police agency located where you reside. California Penal Code 530.6 requires local police agencies to accept and document reports of identity theft from victims who reside within that agency's jurisdiction. However, the agency is not required to investigate incidents of identity theft that have occurred outside of that agency's jurisdiction. The law only requires the agency to document the incident and forward the report to the agency or agencies that have jurisdiction where the incident occurred. The victim is responsible for contacting those agencies to inquire about the status of their complaint.
- Be prepared to provide the officer with any and all documents related to the theft of your identity. This may include documents such as credit applications, receipts, or letters from creditors, collection agencies, or credit reporting agencies. Gathering this information is the responsibility of the victim and should be done before filing a report with the police. Creditors will not release victim identity or account information to investigators. Since your name and other identity information is on the fraudulent account(s) you have the right to receive copies of all documents and information related to the account(s) for use in proving the accounts were fraudulently established and that you were a victim of identity theft.
- Be prepared to be fingerprinted and to have your photo taken as part of the investigative process.

- Contact your local postal inspector if your mail has been stolen or the address of where your mail is delivered was changed without your knowledge or authorization. Complete USPS Form 2016; Mail Theft / False Change of Address. Call one of the numbers below for directions about where to send the form.

Postal Inspector Offices are located in:

- Oakland (510) 251-3013
 - San Francisco (415) 778-5800
 - San Jose (408) 938-4802
- or via the Internet at www.usps.gov/websites/depart/inspect

Notify your creditor or financial institution if your address was changed on credit card or banking accounts and take the following steps:

- Close the account.
- Open a new account and ask that a password be required for inquiries or changes of address.
- If your checks have been stolen or misused.
- Call your financial institution and place a stop payment on the checks.
- Consider closing your current bank account and opening a new account.

Notify the major check verification services:

- National Check Fraud Service (843) 571-2143
- SCAN (800) 262-7771
- TeleCheck (800) 710-9898
- Cross Check (707) 586-0551
- Equifax Check Systems (800) 437-5120
- International Check Services (800) 526-5380

If telephone service has been fraudulently established in your name:

- Contact the phone services provider where the fraudulent account was established, or if applicable the cell phone provider where the account was established.
- If the provider is not able, or refuses, to assist you with resolving your complaint you should contact the following government agencies:
 - California Public Utilities Commission (for local phone service providers) at (415) 703-2782 or via the Internet at www.cpuc.ca.gov
 - Federal Communications Commission (for long distance and cellular providers) at (888) 225-5322 or via the Internet at <http://esupport.fcc.gov/complaints.htm>
 - If your social security number is fraudulently being used for employment purposes contact:
Social Security Administration Fraud Hotline (800) 269-0271
In extreme cases the SSA may issue you a new social security number. However, this may not solve your problem. Included with this informational packet are publications regarding fraudulent use of social security numbers. Please take a moment to read them.
If someone has filed for bankruptcy in your name contact:

U.S. Trustee (local region)

You may locate your local region via the Internet at www.usdoj.gov/ust

How identity information is stolen:

- From thefts of purses, wallets, brief cases, backpacks, etc. containing identity information.
- Mail theft from unsecured mail boxes.
- From business, financial, medical or government computer databases.
- When criminals retrieve unshredded documents and mail, containing identity information, from dumpsters (also referred to as "dumpster diving").
- By purchasing identity information from information brokers.
- By illegally obtaining credit reports.
- By stealing identity information found when criminals commit residential and commercial burglaries.
- When your mail is illegally rerouted from your home or P.O. Box to a different address.
- By stealing identity information via the Internet.
- By purchasing identity information from "inside" sources at banks, schools, medical facilities, DMV, insurance companies, government agencies, etc.

How identity thieves use your information:

- Thieves open new lines of credit and take out new loans using your identity information.
- Thieves open bank accounts using your identity information.
- Thieves impersonate you and pass fraudulent checks through your bank account.
- Thieves impersonate you while committing crimes making you the subject of a criminal investigation.
- Thieves file for bankruptcy using your identity information

How to reduce your risk of being a victim of identity theft:

- Before providing any identity information to a business or person, find out how it will be used, whether it will be shared with others, and the entity's privacy policy. Ask about "opting out" of the sharing of your identity information.
- Closely monitor your bills / statements for accuracy. Dispute, in writing, any inaccurate charges.
- Follow-up with creditors when you don't receive your bills during their normal billing cycle. It may be a sign that an identity thief has rerouted your mail to another address.
- Deposit your mail at the post office in an interior collection box. Don't leave mail in unsecured locations for pick up by the postal carrier.
- Only have mail delivered to a secure mailbox.
Have the post office hold your mail while you are away from your residence or business.
- Do not keep PIN number or password information in your purse, wallet, or organizer.
- Limit the amount of identity information you keep in your purse, wallet, or organizer.
- Avoid using for passwords easy to discover information such as your mother's maiden name, birthday, social security number, or phone number.
- Do not give identity information to anyone with whom you have not initiated contact.
- Shred all documents containing your identity information using a cross cut shredder.
- Secure documents in your home that contain identity information.
- Make your phone number unlisted or only list your name and phone number.
- Limit the release of your name, address, phone number, and other identity information.
- Do not complete personal profile surveys such as those found on new product warranty cards.

Order and review your credit reports at least once per year:

- Equifax (800) 525-6285
- Experian (888) 397-3742
- Trans Union (800) 680-7289

Remove your name from mailing lists:

To have your name removed from direct marketing mailing lists contact

DMA Mail Preference Service

P.O. Box 9008

Farmingdale NY 11735-9008

To have your name removed from direct marketing telephone solicitation lists contact:

DMA Telephone Preference Service

PO Box 9014

Farmingdale NY 11735-9014

or via the Internet at www.the-dma.org

To have your name removed from the three credit bureaus marketing lists, call (888) 567-8688

- Name removed for 2 years if request made by phone
- Name removed for 5 years if request made in writing

To have your name permanently removed from Experian's marketing lists call (800) 407-1088

To have your name permanently removed from an individual organization's mailing list Complete USPS Form 1500

Identity Theft Registry:

The California Department of Justice has Launched a new Identity Theft Registry that will assist victims who are wrongfully identified as criminals due to unlawful use of their identities. Once registered, inquiries to the state criminal history system will return a reply indicating that the individual has been a victim of identity theft and to contact the California Department of Justice for further information. Additionally, the victim may have the Department of Justice notify any individuals or agencies they designate to advise them they have been a victim of identity theft.

Basic registration requires the submission of an application along with fingerprints and court verification that the individual is a victim of identity theft. More information about the registry may be obtained by calling 1-(888) 880-2040, by visiting the Department of Justice Web Site at <http://ag.ca.gov/idtheft/form.php> or by writing to them at:

Department of Justice

PO Box 903417

Identity Theft Registry - Room G210

Sacramento, CA. 94203-4170

Contact the California Office of Privacy Protection

In January of 2002 several California laws took effect addressing the crime of identity theft:

California Financial Code 4002

California Financial Code 22470

California Civil Code 1748.95

California Penal Code 530.8

The new laws require credit grantors and utility companies to furnish identity theft victims with copies of documents associated with accounts opened fraudulently using the victim's identity information. These documents include, but are not limited to, copies of any applications and records of charges associated with the fraudulent account. The information must be provided to

you free of charge within ten business days from when the credit grantor receives your request. The credit grantor may require you to provide your identity information to them, including, but not limited to your name, address, phone number, date of birth, driver's license number, and social security number. Additionally, the credit grantor may require you to send them a copy of the identity theft report you filed with your local police department and also to sign a document authorizing the release of information.

Please contact the California Office of Privacy Protection (C.O.P.P.) at (800) 952-5210 or (916) 323-0637 for further information, forms, and sample letters. You may also contact C.O.P.P. via e-mail at privacyprotection.ca.gov or by regular mail at:

Office of Privacy Protection
California Department of Consumer Affairs
400 "R" Street - Suite 300
Sacramento, CA 95814

Resources:

The following organizations provide prevention information regarding Identity Theft and also offer assistance to victims of Identity Theft. Additionally, they provide information on current legislation regarding privacy rights in addition to Identity Theft legislation:

CALPIRG - <http://www.calpirg.org/>

Privacy Rights Clearing House - www.privacyrights.org

US Privacy Rights Group - www.privacyrights.org/

Current Legislation:

California SB168 - Allows people to restrict access to their credit reports. Would prevent financial service institutions from obtaining credit reports and using them for marketing purposes without a consumer's specific permission. Prevents businesses from printing SSN numbers on any type of identification card or anything mailed to customers. California SB773 - Would give customers of financial institutions more control over how those institutions use and share a customer's identity and financial information ("Opt-In" vs "Opt Out" marketing concept).

Information Brokers:

Some brokers sell public record information to individuals. The City of Palo Alto does not recommend or endorse any of these businesses. This information is provided to you solely as a resource to help you identify where your identity information exists and how much of that information is available to the public.